This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (currently amended) A method for dynamically managing access to a resource in a computer system, the system having a client thereof having an application making an access request for the resource, the method comprising:

initializing a client authorization context for the client using one or more client context initialization routines;

determining, via an application programming interface, based upon dynamic data possessed by the application and a first dynamic policy whether [[a]] said client authorization context is to be updated and, if so, updating said client authorization context, wherein said first dynamic policy is tailored to ~~an~~ said application ~~through which the resource is accessed~~;

invoking an access check routine to determine if the application or client represented by the client authorization context is allowed access to the resource, the application providing said dynamic data and an identifier for the access check to the access check routine for comparison against access control entries;

identifying an access control entry as a callback access control entry; and

in response to identifying the access control entry as a callback access control entry and a match between ~~an~~ said identifier ~~in the client authorization context~~ and an identifier in the callback access control entry, automatically invoking, via said application programming interface, an application-defined dynamic access check routine that performs the access check for the application based upon said dynamic data and a second dynamic policy in the callback access control entry for the application, wherein said second dynamic policy is tailored to said application and said dynamic data includes authorization policy data stored in [[a]] said callback access control entry and/or run-time data managed by the application.

2. (original) A method according to claim 1, wherein said first dynamic policy defines flexible rules for determining the client authorization context and wherein said second dynamic policy defines flexible rules for purposes of determining access privileges.

3. (original) A method according to claim 1, further comprising computing the client authorization context after a request for a resource is received from the client and updating said client authorization context according to said determining.

4. (original) A method according to claim 1, further comprising:

comparing the client authorization context of the client to at least one access control entry of an access control list.

5. (canceled)

6. (canceled)

7. (original) A method according to claim 1, further comprising registering with a resource manager, an application-defined routine for determining dynamic groups.

8. (original) A method according to claim 1, further comprising registering with a resource manager, an application-defined routine for determining dynamic access checks.

9. (previously presented) A method according to claim 1, wherein said application-defined dynamic access check routine supplements a determination of access rights based upon static data and policy.

10. (previously presented) A computer readable storage medium having computer executable instructions stored thereon that when executed by a computer cause the computer to implement the method of claim 1.

11. (canceled)

12. (currently amended) A computer readable storage medium having computer executable instructions stored thereon that when executed by a computer cause the computer to carry out a method for dynamically updating a client authorization context in a computer system having a client thereof having an application making an access request for a resource, the method comprising:

computing a client authorization context after the request for the resource is received from the client;

determining, via an application programming interface, based upon dynamic data possessed by the application and a first dynamic policy whether said client authorization context is to be updated and, if so, updating said client authorization context, wherein said first dynamic policy is tailored to ~~an~~ said application ~~through which the resource is accessed~~;

~~updating said client authorization context according to said determination;~~

invoking an access check routine to determine if the application or client represented by the client authorization context is allowed access to the resource, the application providing said dynamic data and an identifier for the access check to the access check routine for comparison against access control entries;

identifying an access control entry as a callback access control entry; and

in response to identifying the access control entry as a callback access control entry and a match between ~~an~~ said identifier ~~in the client authorization context~~ and an identifier in [[a]] the callback access control entry ~~for the application~~, automatically invoking, via said application programming interface, an application-defined dynamic access check routine that performs the access check for the application based upon said dynamic data and a second dynamic policy in the callback access control entry for the application, wherein said second dynamic policy is tailored to said application and said dynamic data includes authorization policy data stored in [[a]] said callback access control entry and/or run-time data managed by the application.

13. (previously presented) A computer readable storage medium according to claim 12, the method further comprising:

comparing the client authorization context to at least one access control entry of an access control list.

14. (canceled)

15. (canceled)

16. (canceled)

17. (canceled)

18. (previously presented) A computer readable storage medium according to claim 12, the method further comprising registering with a resource manager, an application-defined routine for determining dynamic groups.

19. (previously presented) A computer readable storage medium according to claim 12, the method further comprising registering with a resource manager, an application-defined routine for determining dynamic access checks.

20. (previously presented) A computer readable storage medium according to claim 12, the method further comprising comparing data to a client authorization context determined based upon static data and policy before determining whether the client authorization context is to be updated.

21. (previously presented) A computer readable storage medium according to claim 12, wherein said application-defined dynamic access check routine supplements a determination of access rights based upon static data and policy.

22. (currently amended) A computer readable storage medium having computer executable instructions stored thereon that when executed by a computer cause the computer to perform a method of dynamically managing access to a resource in a computer system, the system having a client thereof having an application making an access request for the resource, the method ~~implemented by the computer~~ comprising:

computing a client authorization context after the access request for the resource is received from the client;

determining, via an application programming interface, based upon dynamic data possessed by the application and a first dynamic policy whether said client authorization context is to be updated and, if so, updating said client authorization context, wherein said first dynamic policy is tailored to said application;

comparing the client authorization context ~~of the client~~ to at least one access control entry of an access control list to determine if the application or client represented by the client authorization context is allowed access to the resource;

the application providing dynamic data to an access check routine for comparison against access control entries for identifying an access control entry as a callback access control entry; and

in response to identifying the access control entry as a callback access control entry, ~~determining, via an application programming interface, based upon dynamic data and dynamic policy whether said callback access control entry bears on said access request, and~~ automatically invoking, via said application programming interface, an application-defined dynamic access check routine that performs the access check for the application based upon said dynamic data and a second dynamic policy in the callback access control entry for the application, wherein said second dynamic policy is tailored to said application and said dynamic data includes authorization policy data stored in [[a]] said callback access control entry and/or run-time data managed by the application.

23. (canceled)

24. (previously presented) A computer readable storage medium according to claim 22, wherein said access check routine is invoked automatically when there is a match between an identifier in the client authorization context and an identifier in the callback access control entry.

25. (previously presented) A computer readable storage medium according to claim 22, wherein said application-defined dynamic access check routine supplements a determination of access rights based upon static data and policy.

26. (currently amended) For an application in a computer system having a resource manager that manages and controls access to a resource, a computer readable storage medium having computer executable instructions stored thereon that when executed by [[a]] the computer system causes the computer system to carry out a method for dynamically updating a client authorization context in the computer system, the

computer system having a client thereof having an application making an access request for a resource, the method comprising:

initializing a client authorization context for the client;

updating said client authorization context based upon dynamic data possessed by the application; and

carrying ~~carry~~ out a dynamic authorization callback mechanism to determine if the application or client represented by the updated client authorization context is allowed access to the resource, the dynamic authorization callback mechanism providing ~~that provides~~ extensible support for application-defined business rules via a set of APIs and DACLs including a dynamic groups element, ~~which enables an~~ and said dynamic groups element enabling said application to assign temporary group membership, based on dynamic factors, to [[a]] said client for the purpose of checking access rights, wherein said dynamic groups element and a dynamic access element utilize dynamic data that includes authorization policy data ~~stored in callback access control entry~~ and/or run-time data managed by the application.

27. (currently amended) A computer readable storage medium ~~having computer executable instructions stored thereon that when executed by a computer causes the computer to carry out a dynamic authorization callback mechanism~~ according to claim 26, further comprising carrying out a dynamic access check element~~, which~~ that enables ~~an~~ said application to perform dynamic access checks, via DACLs and APIs, said dynamic access checks being customized to the application.

28. (currently amended) A computer readable storage medium ~~having computer executable instructions stored thereon that when executed by a computer causes the computer to carry out a dynamic authorization callback mechanism~~ according to claim 26, ~~wherein~~ further comprising registering said dynamic groups element and [[a]] said dynamic access element ~~are registered~~ with the resource manager upon initializing the resource manager and storing said authorization policy data in a callback access control entry.

29. (canceled)

30. (canceled)

31. (canceled)

32. (canceled)

33. (currently amended) A computer readable storage medium having computer executable instructions stored thereon that when executed by a computer causes the computer to provide dynamic authorization of an application in a computer system based upon application-specific or business rules that incorporate dynamic data, the dynamic data including an identifier for identifying whether a dynamic access check callback function should be invoked for conducting said dynamic authorization of said application, data from client operation parameters, authorization policy data stored in a callback access control entry, and any other authorization policy data managed, computed or retrieved by the application, the computer executing said computer executable instructions to perform the steps of:

the application using an initialization routine to register with a resource manager dynamic group functions that enable the application to assign temporary group membership based upon transient or changing factors to a client for the purpose of checking access rights and to register with said resource manager dynamic access check callback functions that enable the application to perform customized procedures for checking access rights based on said transient or changing factors;

adding said dynamic access check callback functions to the resource manager's registered callback list; and

~~automatically invoking a registered dynamic access check callback function by access check application programming interfaces that initialize a client authorization context from a system level authorization context or a user's security identifier, whereby~~ when a user attempts to connect to the application, automatically invoking a ~~the~~ registered dynamic access check callback function to provide said customized procedures for checking access rights based on said transient or changing factors ~~is invoked such that the client context is augmented with client contextual data dynamically computed using said dynamic data~~.

34. (currently amended) A computer readable storage medium according to claim 33, wherein ~~said~~ a user's security identifier is used for an access privilege check of said application.